



## **EMAIL USE POLICY FOR CONTRACTORS**

**Scope.** This policy applies to all contractors, vendors and partners ("Contractors") of Red River Technology LLC and its affiliates ("Red River") who are assigned a Red River email address ("Red River Email").

**Purpose.** The purpose of this policy is to describe the permitted uses of Red River Email by Contractors. This policy does not replace or supersede any separate agreements between Red River and Contractor or Contractor's employer.

**Policy.** Contractors may only use their Red River Email for Red River business purposes. Contractors must not use Red River Email for any personal reasons or non-Red River business. Contractors must not use any personal email (e.g., Yahoo, Hotmail or Gmail) for Red River business. Contractors may not set their Red River Email to automatically forward to any other email address and will only forward emails received to its Red River Email as necessary and required for Red River business purposes. Contractors may not forward any emails with Red River Confidential Information to personal email or employer provided email addresses, if any. Red River Email must not be used to communicate and/or create improper and/or illegal messages (such as obscene, derogatory, defamatory, or otherwise inappropriate messages).

Contractors may not represent that they are employees of or otherwise make contractual commitments on behalf of Red River. Contractors must abide by security requirements provided by Red River, including password requirements and training. Contractors must be vigilant to detect emails that may carry malware or phishing attempts.

All Red River Email and computer systems with access to Red River Email must be password protected. The password must be changed at least every 90 days and consist of at least eight (8) characters including, at a minimum, the following:

- Lower case characters
- Upper case characters
- Numeric characters
- Special characters (!@#\$%^&\*)
- Must NOT contain the username

You may not reuse the prior four passwords. Your system may automatically lock-out following five (5) attempts at password entry. This lock-out will require a call to the Help Desk at 1.603.442.5502 or 1.888.855.7722 before you can attempt another login. You may not share passwords through verbal communication, email or any other method. You may not write down your password.

Red River reserves the right to access, monitor, retrieve, review, save, archive, and disclose communications including both data and information on the system, including all emails. You are responsible for the content of your communications. **DO NOT USE RED RIVER EMAIL OR RED RIVER SYSTEMS WITH ANY EXPECTATION THAT YOUR USE WILL BE CONFIDENTIAL OR PRIVATE FROM COMPANY REVIEW.**

No sensitive information may be sent via unsecured email. Credit card information may only be transmitted via verbal communication and Red River's Navision. When exchanging other sensitive information, Contractors must use Mimecast Secure Send. This capability allows for secure transmittal of content via your email box. The recipient will get a link and login to the Mimecast allowing them to retrieve the message via Mimecast's encrypted portal.

Red River Contractors may be required to make use of government furnished equipment ("GFE") when working in public sector customer environments. To maintain a secure computing environment, you must observe the following:

- Do not setup Outlook on GFE to access your Red River Email. Doing this will leave a copy of your mailbox on the provided GFE.
- If you need to use Red River Email, access it via Office 365 Outlook Web Access. Ensure you do not save your login to O365 in the web browser, don't leave the computer unattended and logged into your email and make use of Internet Explorer "InPrivate" browsing when logging in to limit information being left on the GFE.
- Do not transfer any work files onto the GFE that do not pertain to that specific public sector customer or that reveal any Red River proprietary information.

Contractors must comply with all security and acceptable use policy requirements of the public sector customer they are working with. Examples include, but are not limited to, the following: use of USB drives, password requirements, social media access, use of device cameras and installation and/or downloading of software.

In connection with the services to be provided by Contractor, Red River may disclose to the Contractor technical, financial and/or other information, material, or data which is written, oral or in any other form, electronic or otherwise which is considered confidential and proprietary ("Confidential information"). Contractor agrees to use the same degree of care and diligence to protect Confidential Information from disclosure to others as it employs or should reasonably employ to so protect its own information of like confidence (but in no event less than reasonable care), and to promptly notify Red River upon discovery of any loss or unauthorized disclosure of the Confidential Information.

**Acknowledgment.** I acknowledge receipt of this Email Use Policy for Contractors. I have read and agree to be bound by it.

---

Printed Name



---

Signature

---

Name of Contractor's Company/Employer

---

Date